PATENT APPLICATION
DOCKET NO. AUD04-004-5

METHOD FOR COMPUTER NETWORK OPERATION PROVIDING BASIS FOR USAGE FEES

INVENTOR:

François Xavier Nuttall

METHOD FOR COMPUTER NETWORK OPERATION PROVIDING BASIS FOR USAGE FEES

FIELD OF THE INVENTION

The present invention relates to computer networks for data transfer and to

5   monitoring use of such data for example for fee accounting for usage rights.

BACKGROUND OF THE INVENTION

Publishers of information in digital form desire to prevent the unauthorized and unaccounted distribution or usage of electronically published materials. Electronically published materials are typically distributed in a digital form and

10   recreated on a computer based system. Audio and video recordings, computer programs, books, and multimedia are examples of works that are suitable for publishing electronically. The sales revenue for companies in the electronic publishing and information systems industries includes payments based on an accounting for delivery of information in digital form, for example the sale of an

15   audio CD at a retail outlet. Any unaccounted distribution of a work results in decreased revenue to the distributor and decreased royalty for the owner of usage rights in the work. For example, being able to copy an audio recording CD to another digital medium from which the audio can be retrieved and played circumvents payment for distribution from which royalty for copyright may have

20   been due to the owner of rights in the work.

Owners of rights in electronically published works also desire to prevent the unauthorized and unaccounted distribution or usage of such materials. When records of the distribution and usage of a work are held exclusively by the distributor, falsification of records results in increased profit for the distributor and

25   loss of royalty income for the owner of rights.

Unauthorized and unaccounted distribution can be curbed by preventing unauthorized copying of the work onto digital storage media and unauthorized transmission of the work over computer networks. Unauthorized and unaccounted usage can be curbed by preventing storage of the work for reuse or by monitoring

30   the use of stored copies.

Existing systems and methods for preventing storage, transmission, and

Case AUD04-004-5

unmonitored use of digital works place a heavy burden of cost on the consumer desiring access to a work in digital form. The continued expansion of publication and use of works in digital form cannot remain within the policies for intellectual property protection (such as providing incentives to authors and publishers) without

5   systems and methods for computer network operation that provide an accurate basis for usage fees.

SUMMARY OF THE INVENTION

A system for the control of distribution and use of digital works includes a distribution and usage reporting mechanism for accurately calculating fees

10   associated with such distribution and use. The system operates according to a method for transferring data from a content providing node to a content requesting node. The method includes the steps of: (a) transmitting a first request to the content providing node, the first request for notifying an authorizing node; (b) receiving a permit from the authorizing node in response to the notification; (c)

15   determining a file name in response to the permit; (d) transmitting to the content providing node a second request comprising the file name; (e) transmitting to an event reporting node a first report in response to receiving the permit; (f) receiving data from the file; and (g) transmitting to the event reporting node a second report in response to receiving the file.

20   By obtaining the permit without direct communication from the content requesting node and the authorizing node, manipulation of the authorizing node by the content requesting node is prevented. The content requesting node has an incentive to manipulate the authorizing node in order to receive unlimited authorization. The content providing node has an incentive to maintain proper

25   authorization because revenues to the content providing node may be based on the number of authorized transfers.

Although a work may be identified in the request received at the content providing node, the content providing node may be prevented from obtaining information leading to the filenames that comprise the work. The content providing

30   node may have an incentive to provide free transfers of the work for other commercial or personal use; however, by determining the file name in response to

Case AUD04-004-5

the permit and preventing access to the permit from the content providing node, the content providing node cannot identify particular files that correspond to a particular work.

By transmitting reports from the content requesting node to an event

5   reporting node, modification of data transfer reports by the content providing node is prevented. Accurate records provide basis, for example, for fees payable to owners of rights in the work.

By transmitting a first report prior to data transfer and a second report after data transfer, a duration of the usage of the data may be used as a basis, for

10   example, for revenues to distributors and payments to owners of rights. Falsification of the duration of usage by the content requesting node is prevented.

BRIEF DESCRIPTION OF THE DRAWING

Fig. 1 is a block diagram of a network in one embodiment of the present invention.

15   Fig. 2 is a data flow diagram for a portion of the network of Fig. 1 that, *inter alia*, creates content files on a content providing node.

Fig. 3 is a data flow diagram for a portion of the network of Fig. 1 that, *inter alia*, satisfies a data transfer request.

Fig. 4 is a data flow diagram for a portion of the network of Fig. 1 that, *inter*

20   *alia*, accomplishes payments, for example, to owners of rights in data transferred.

Fig. 5 is a table of outcomes for lost transmissions of reports.

Fig. 6 is a functional flow diagram for a portion of a method of validating a request by an authorizing node.

Fig. 7 is a functional flow diagram for a portion of a method of creating a

25   permit by an authorizing node.

Fig. 8 is a functional flow diagram for a portion of a method of validating a permit by a content requesting node.

Fig. 9 is a functional flow diagram for a portion of a method of reporting, by a content requesting node, a start of data transfer.

30   Figs. 10 through 12 are functional flow diagrams for portions of a method of obtaining and using content files and reporting a summary of data transfer.

Fig. 13 is a memory map of a data structure of a map file of the present invention.

Fig. 14 is a memory map of a data structure of a header of a content file of the present invention.

Fig. 15 is a memory map of a data structure of a request of the present invention.

Fig. 16 is a memory map of a data structure of a permit of the present invention.

Fig. 17 is a memory map of a data structure of a start report of the present invention.

Fig. 18 is a memory map of a data structure of a summary report of the present invention.

Fig. 19 is a memory map of a data structure of an access report of the present invention.

Fig. 20 is a memory map of a data structure of a debit report of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Data transfer in the present invention is illustrated among computer systems using a communication network. A communication network of the present invention includes at least one computer system at each of several network nodes. Each node is coupled by a link from time to time for communication with other nodes of the network. Each link includes conventional computer communication technology of the type including, for example, local area, wide area, dedicated telephone, or satellite services and including conventional data communication hardware and software. The popular computer networks known as the Internet, World Wide Web, and National Information Infrastructure are examples of such a communication network having nodes possibly at physically separate locations and addressed by a node address, for example a uniform resource locator (URL), a name from a domain name system (DNS), or an Internet Protocol address (IP).

Communication network 100 of Fig. 1 includes computer systems, each shown in a block, that communicate for data transfer. Communication of

messages is illustrated by one or more lines between blocks, though it is apparent that one communication link between any two blocks is sufficient for any number of message lines. Practice of variations of the invention is independent of whether such a link is maintained continuously, as in a dedicated line, or is maintained for

5   the duration of the message as in some public multiple access facilities.

Communication technology provides known mechanisms and computer software for message transfer. This technology surrounds the message content data with other data that provide a mechanism for various purposes including tracking messages, synchronizing equipment, and assuring accurate and secure

10   transfer of message content data. In the description that follows, digital works are transferred between nodes. The term "content," therefore, refers to a digital work or a portion thereof.

Network 100 includes content acquisition node 102, content managing node 104, provider preparation node 106, content providing node 108, content

15   requesting node 110, authorizing node 112, banking node 114, event reporting node 116, and reconciling node 118.

In operation, for content to be transferred on request to any of perhaps millions of content requesting nodes, the content is first received from a source and formatted for storage on one or more of perhaps thousands of content

20   providing nodes. Initially, a content developer, publisher, or distributor provides digital works, for example multimedia files, to content acquisition node 102 for encoding in a format efficient for storage and access by content managing node 104. Content is conveyed on line 130 as it becomes available for management by content managing node 104. Content from content managing node 104 is

25   conveyed on line 132 and then made unique to each content providing node 108 by formatting processes performed by provider preparation node 106. Content providing node 108 receives content from time to time from provider preparation node 106 on line 134.

To request a data transfer in a preferred embodiment for the Internet, a user

30   or consumer at content requesting node 110 uses a network browser, such as Microsoft Internet Explorer, and follows an Internet link (clicks on a portion of an HTML file display), causing a message in HTTP format to be conveyed on line 136

Case AUD04-004-5

to content providing node 108. Content providing node 108 forwards the request on line 138 to authorizing node 112. If the request is valid, authorizing node 112 creates a permit and sends it on line 146 to content requesting node 110. A permit is a message created to uniquely respond to the request from a particular
5   content requesting node. Using portions of the permit, content requesting node 110 requests on line 136 particular files from content providing node 108. In response, such particular files are conveyed on line 148 to content requesting node 110, completing the data transfer.

Accounting for the above described transfer of content includes, for
10   example, receiving payment from the user of content requesting node 110, making payment for distribution services to at least the operator of content providing node 108, and making payment to one or more owners of rights in the content. These accounting transactions find accurate basis in a reconciliation of reports from a variety of network nodes and reported at separate times during the data transfer
15   process. For example, when authorizing node 112 receives the request and queries an access authority data base on content managing node 104 via lines 140 and 142, content managing node 104 logs the query and reports the log on line 156 from time to time to reconciling node 118. With knowledge of the identity of content requesting node 110, an identity of the user, and a price of the requested
20   work for a requested purpose (for example, copy or preview), authorizing node confirms a debit of an account kept on banking node 114 by messages conveyed on line 144. Banking node 114 logs the debit and reports the log on line 154 from time to time to reconciling node 118. When the data transfer begins and again when at least some of the data has been transferred, content requesting node 110
25   reports on line 150 to event reporting node 116. Event reporting node 116 logs the events and from time to time reports the log on line 152 to reconciling node 118. By comparing reports received on lines 152, 154, 156, and possibly 158 (from content providing node 108), reconciling node distinguishes valid complete data transfers from incomplete transfers and from events that could indicate
30   intentional interference with the integrity of network 100. For each valid complete transfer, reconciling node allocates revenues generated from the debits of users' accounts, discussed above with reference to line 144. Reconciling node then

initiates funds transfers with messages to banking node 114 on line 160 for payments of, for example, distribution fees and royalties.

Each node of network 100 may represent more than one conventional computer system that performs, *inter alia*, methods of the present invention.

5   Multiple computers or multiple data storage devices may be necessary for maintaining a particular node's functions operational in periods of high network traffic. Such multiple computers may be at various physical locations, provided that only one network node address (for example, an IP address) is associated with each node.

10   A method of the present invention for preparing content for storage on a content providing node includes separation of content and map information. When content is divided for convenience into several files in a conventional file storage system, map information identifies the particular files from the entire inventory on the storage system and the order of presentation of the files for reconstituting a

15   particular work. Separation of content and map information facilitates security measures without unduly compromising rapid provision of a work or performance of a work on a content requesting node.

For example, as shown in Fig. 2, content acquisition node 102 encodes (using conventional data formatting and compression technology) contract items

20   associated with the work and encodes the work itself. When the work is primarily an audio recording, contract items may additionally include: name of the album, producer, label, publisher, mail order company, publishing year, bar code, album and track distribution levels, title of a track, performers, authors, composers, ISRC code for the title, language, track number, duration, extract start and end times,

25   number of allowed copies, price to preview (listen), price to make copy, rights collecting societies, authorized distribution areas, album cover picture, liner notes, other graphics, music style, associated country, and possibly pictures associated with the recording and text to be shown while the work is being played. Receiver processes 204 and 206 (using conventional communication and data storage

30   technology) on content managing node 104, receive the encoded contract items and content and store each respectively on access authority data base (AADB) 208 and content masters store 210.

When a particular content providing node 108 is identified, works to be provided by that node are selected from content masters store 210 and scrambled by process 214 (using conventional data security technology). Scrambling is a preferred (though weak) form of encryption that allows some security without

5 unduly burdening data transfer or use of the work when requested. The scrambled result of a work is combined with a header, which includes encrypted data from access authority data base 208, to form one or more content files. Content files 217 are transferred for storage on store 216 of content providing node 108.

Process 212 prepares map files 218 for transfer and storage on store 216.

10 Descriptors of the work, of the content files, and of content providing node 108 are obtained from AADB 208 and formatted and encrypted by process 212 (using conventional data formatting and encryption technology). Some or all of the descriptors, alone or in combination, may be subject to rigorous encryption. The map file permits content file locations to be random or at least unpredictable in

15 store 216, substantially decreasing the likelihood of unauthorized access without the system performance penalties associated with encrypting a content files 218 on store 216.

In a preferred embodiment for an audio recording, the map file includes a version number of a group of content files and a node address and pathname to

20 each content file of the group. The node address corresponds to the unique node address of the content providing node for which content files are being prepared. Each node address and pathname is encrypted separately. Each content file of the group provides a different level of sound quality for the same audio material. Different levels of quality provide, for example, flexibility in meeting the audio

25 fidelity of different content requesting nodes. Fig. 13 illustrates an example map file data structure 1300 when instantiated in memory at provider preparation node 106. Fig. 14 illustrates an example data structure 1400 of a header of a content file when instantiated in memory at provider preparation node 106.

Content files 217 and map files 218 are organized for convenient access on

30 store 216 using a conventional file system such as a directory system, shadowed physical drives, or a RAID system.

As indicated by ellipsis in Fig. 2, many content acquisition nodes may supply

content to content managing node 104. Many content providing nodes may be supplied with content files from content managing node 104. Due to differing security and traffic support requirements, it is preferred to operate network 100 with physically separate nodes 104 and 106. In a variation, the functions of nodes

5   104 and 106 may be combined on one node or combined with content acquisition node 102.

    Various methods of the present invention for data transfer use to advantage (a) the cooperation of several network nodes, (b) linking a request through a registered node, (c) creating a permit using data from multiple sources, (d) using

10   encryption, current time of day, or encryption keys based on unique properties of a node, and/or (e) providing unique structures and separate access to content files and map files. These features, *inter alia*, accomplish validating the request, validating the permit, and validating the data transfer operation itself. When validation is unsuccessful, data transfer is stopped, preserving the integrity of

15   network 100. The integrity of network 100 may be compromised by unauthorized copying, transfer, or use of a digital work.

    For example, as shown in Fig. 3, a data transfer begins at content requesting node (CRN) 110. There a consumer or service user obtains a listing of titles, each title for a digital work. Process 302 (using a conventional browser and

20   operating system) responds to user input, for example a mouse switch closure ("click") when an on-screen cursor points to a portion of an HTML page identifying a title, and in the conventional manner generates a message 303 to content providing node (CPN) 108. Process 304 (using conventional HTTP message technology) forwards the request 305 to authorizing node (AN) 112. Fig. 15

25   illustrates an example request data structure 1500 when instantiated in memory at authorizing node 112. In a variation, process 304 determines the price to be billed for the request type and title and includes price and price currency with the forwarded request. Price information is stored in file 306 which is available for editing by the operator of content providing node 108. In a preferred embodiment,

30   validate payment process 310 obtains price information via the associated map file from each content file after the validity of the request has been determined.

    Process 308 validates the request by denying further processing to requests

that do not meet predetermined criteria. In one variation, shown in Fig. 6, process 308 includes the steps beginning at step 600. At step 602, the node address of content providing node (CPN) 108 is obtained from access authority data base (AADB) 208. At step 604, the CPN node address as provided in request 305 is

5   compared to the CPN node address as provided from AADB 208. If a match is found, control passes to step 606, else to step 608 where the request is ignored. At step 606, the node address of the calling page (which contains the link that was followed by process 302) is compared to the CPN node address provided by AADB 208. If a match is found, the request is considered valid and control passes to

10   process 310, else to step 608 where the request is ignored.

Process 310 (using conventional data base and communication technology) validates payment by the user by confirming that the user (via pay price process 310) has made a proper debit on the user's account. If a debit cannot be confirmed, request 305 is ignored. If confirmation of the debit transaction is

15   successful, control passes to process 312.

Process 312 creates a permit by combining information from more than one source. In one variation, shown in Fig. 7, process 312 includes the steps beginning at step 700. At step 702, a map file 315 for the requested content is obtained either from the request or from store 216 on content providing node 108.

20   At step 704, content providing node address, content price, and price currency are obtained from request 305. At step 706, local date and time are obtained from the authorizing node 112. These data items are arranged, for example, in data structure 1600 instantiated in memory of authorizing node 112, as illustrated in Fig. 16. At step 708 some or all data in permit data structure 1600 are encrypted

25   to provide permit 313. At step 710, permit 313 is sent to content requesting node 110.

Process 314 validates the permit by stopping the transaction for permits that do not meet predetermined criteria. In one variation, shown in Fig. 8, process 314 includes the steps beginning at step 800. At step 802, that portion of the

30   permit that is encrypted is decrypted. At step 804, the syntax of each content file location (content.CPN.node address.pathname) is checked. The several pathnames in the permit provide ready access to the content file matching the sound quality

level specified in request 305 (see Fig. 15, request.sound.quality). If the syntax
check fails, control passes to step 810 to stop the transaction. Otherwise control
passes to step 806 where the content requesting node address provided in permit
313 is compared to the node address of content requesting node 110. If no

5   match, control is transferred to step 810. If a match is found, control passes to
step 808, the current date and time on content requesting node 110 is compared
to the date and time value stamped by authorizing node (AN) 112 on permit 313
(AN.date.time). If the current time is more than a predetermined amount (for
example, 5 minutes) after AN.date.time, then control passes to step 810 and the

10   transaction stops. Otherwise, control passes to step 812 and, in due course, to
process 316.

    Process 316 reports the start of a data transfer between content providing
node 108 and content requesting node 110. Generation of the report may occur
before data transfer actually starts or during an initial phase of data transfer. A

15   start report is made to one or more event reporting nodes as specified by a list on
content providing node 108. The report is transmitted by packet message
techniques on a separate port so as to avoid interference with the data transfer
itself which may be underway on another port. The two ports may share the same
communication hardware such as a single line to an Internet Service Provider, as is

20   well known in applications of TCP/IP. For other communication hardware and
software configurations, concurrent ports may be arranged on two or more
hardware communication links.

    In one variation, shown in Fig. 9, process 316 includes the steps beginning
at step 900. At step 902, one or more event reporting node addresses are

25   obtained from list 318 on content providing node 108. At step 904, a port is
opened for each event reporting node on list 318. In a preferred embodiment,
ports 1000 through 1016 are used, although other port numbers may be
equivalently accommodated by the communication software on content requesting
node 110. If no event reporting node successfully responds after attempts have

30   been made to couple it for communication, then either the transaction is stopped or
the transaction continues without the capability to generate reports. At step 906,
a port is opened for reporting to content managing node 104, using the next

available port number from the range 1000 through 1016. At step 908, information from request 305 is obtained and placed in a data structure in memory. Fig. 17 illustrates a start report data structure 1700 when instantiated in memory at content requesting node 110. For data structure 1700, such data includes the

5   content requesting node address, the username and password, and the price, currency, and specified sound quality. At step 910, data from permit 313 is added to the start report data structure. For data structure 1700, such data includes the content file location for the specified sound quality level, i.e. a corresponding content.CPN.node.address.pathname.quality.level. At step 912, data from the

10   content file header is added to the start report data structure. For data structure 1700, such data include the title, artist, copyright, duration, ID.code.type (whether ISRC, ISWC, or etc.), the ID.code.number, the content providing node address, and a file number (a serialized number assigned by encoding process 202). At step 914, local values of the content requesting node are added to the start data

15   structure. For data structure 1700, such values include a transaction number for discriminating reports from the same user, the current date and time, an encryption key unique to the content requesting node, and values from which the country in which content requesting node 110 is located. These later values include in one variation of the present invention, the time zone, the language identified by the

20   operating system of node 110 and the keyboard identified by the operating system of node 110. Country location is important to allocating royalties under the laws that vary from one jurisdiction (country) to another. At step 916, the report is placed in final format using conventional techniques and at step 918 it is sent to each event reporting node, for example node 116, and to content managing node

25   104.

Process 320 obtains and uses the requested content files. After a content file header has been received by process 320, the transaction may be stopped if contents of the header do not compare favorably with the permit. In one variation, a summary report is prepared before data transfer of all requested files is complete.

30   In a second variation, a duration of use of the files is measured and reported in a summary report, prepared and sent after all files have been received or usage is determined to be substantially completed. In the later case, shown in Fig. 10,

13

process 320 includes the steps beginning at step 1000. At step 1002, a port is opened for content provider node file transfer (in addition to ports opened for reporting as discussed above). At step 1004, the header of the requested content file is obtained. The pathname to this content file is provided in permit 313 for a corresponding sound quality of content requesting node 110. After decrypting the pathname itself, at step 1006, the header of the specified content file is decrypted. At step 1008, if the content providing node address in the obtained content file header does not match the content providing node address as permitted, the transaction stops at step 1010. Otherwise, control passes to step 1012.

At step 1012, the usage mode as permitted is compared to the usage mode as requested. The user specifies a usage mode at the time of picking a title for a digital work to facilitate calculation of an appropriate price. For example, in many cases, the price for previewing a work (as in listening to a portion of an audio work) is less than the price for making a copy of a work for unlimited use. If the requested and permitted usage modes both indicate a copy is to be made, that is, the data transferred will be stored for repeated use, then control passes to step 1202 on Fig. 12. Otherwise, control passes to step 1102 of Fig. 11. Steps 1102 through 1108 obtain all subsequent blocks of the requested content file and, after each block is received, perform the digital work according to the data in that respective block. Unscrambling of the data may be required. Performance or preview may be, for example one or more of the following: playing audio, showing visual, performing multimedia, or executing computer program digital works. For example, when an audio file is being received, unscrambling is performed and the resulting data may be played without interruption.

At step 1110, information from several sources is combined to form a summary report. One purpose of the summary report is to indicate for purposes of reconciliation, the duration the digital work was being performed. Fig. 18 illustrates a summary report data structure 1800 when instantiated in memory at content requesting none 110. For summary report 328, data items from start report structure 1700 (having the same names) are formatted in summary report data structure 1800. At step 1112, the summary report is sent through ports opened in steps 902 and 904 to one or more event reporting nodes. The

transaction is completed at step 1114.

If at step 1012, a copy of the work has been permitted, control passes to step 1202. At step 1202, a destination file for receiving the digital work is opened on the content requesting node 110. At step 1204, an encryption key is prepared

5   using conventional data security technology. At step 1206, the content file header is obtained and written to the destination file. At steps 1208 through 1214, each block of the requested content file is obtained, encrypted, and written to the destination file. At step 1216, the destination file is closed. At step 1218 the transaction is completed.

10   From time to time, reports are generated by various nodes for checking the integrity of network 100 and for allocating revenues received by debiting user accounts as described with reference to Fig. 3 process 310. Five reports are provided in network 100. Access report 332 is provided by content managing node 104 from queries of AADB 208 initiated by authorizing node processes 308

15   through 312. Fig. 19 is a memory map of data structure 1900 of an access report record when instantiated in memory of content managing node 104 or reconciling node 118. Report 342 is provided by banking node 114 from debit transactions requested by process 310 of authorizing node 112. Fig. 20 is a memory map of a data structure of a debit report record when instantiated in memory of banking

20   node 114 or reconciling node 118. Reports 326 and 328 respectively provide the start and summary information from content requesting node 110. Data structures 1700 and 1800 correspond to a single record of the start report and summary report respectively when instantiated in memory of reconciling node 118. Finally, report 336 may be generated by content providing node 108.

25   Each report consists of multiple records, each record having multiple fields. Because these reports have some fields in common, comparison of the data in identical fields ("reconciliation") provides the basis for distinguishing valid complete transactions from interrupted and unauthorized transactions. For example, an access report record 1900, debit report record 2000, start report 1700, and

30   summary report 1800 each include a tracking field for the value: request.CRN.node.address.transaction.number. By noting whether all four records having the same value for this tracking field have been received at reconciling node

118, conclusions about network integrity and allocation of funds can be reliably made.

A method for reconciling reports of the present invention includes accommodations for high volume event report processing. In addition, reconciled reports may be used to identify nodes having suspect operations and thereby provide a way of detecting unauthorized copying and use of digital works.

In combination with the operation of the AADB 208, unauthorized use may be blocked. For example, if unauthorized transactions frequently involve the same content providing node address, that node address may be deleted from the list of registered content providing nodes by an appropriate operation on AADB 208. When a content requesting node makes a request through the link at the offending content providing node address, the request will be denied at the authorizing node.

An example of a reconciliation method of the present invention is illustrated in Fig. 4. Event reporting node 116 receives start report 326 and summary report 328 at high traffic levels from numerous content requesting nodes. Each report is logged as an event by process 402 using conventional database technology. Logged events are stored for a time in events data base 404. Synchronization of multiple parallel event reporting nodes may result in additional database transactions by event reporting node 116 as to records in events data base 404.

From time to time records from events data base 404 are provided to reconciling node 118. Process 406, using conventional data base technology, accomplishes the comparison of records having one or more respective field values that are identical. In one variation, the tracking field is used exclusively. Table 502 in Fig. 5 identifies results of reconciliation for several combinations of reports being reconciled. If for a given tracking field value (or at a given time, date, content requesting node, and content providing node), reports A 332, B 342, C 326, D 328, and possibly E 336 have been logged, then a group of messages accomplishing a normal request and payment for data transfer can be inferred to have been completed successfully. Allocation of earnings by process 408 follows the identification of such a reconciliation result.

If on the other hand, no report is received for reconciliation having the given common field values, then it can be suspected that software on one or more nodes

of network 100 may have been manipulated, compromising network integrity. Due to the large number of content requesting nodes and the lack of physical controls that could protect software on such nodes from being manipulated, it is likely that at least some of the failures to receive all expected reports may be a consequence

5 of content requesting node software manipulation. In cases 508 and 510, some or all requested data transfer might have been successful; however, allocation of earnings may not be justified when there remains a possibility that a user of the respective content requesting node may insist that the debit to his account be reversed.

10 Allocation of earnings by process 408 is consummated by generating, according to conventional banking messaging and data base technology, requests for funds transfer by process 410 in banking node 114.

As described in detail above, network 100 overcomes the problems of the prior art and provides a basis for accurate allocation of earnings to the owners of

15 rights in digital works stored on systems of the present invention or transferred according to methods of the present invention. These and other benefits are provided with lesser system performance penalties than heretofore possible.

The present invention has been described in the preferred embodiments. Several variations and modification shave also been described and suggested.

20 Other embodiments, variations, and modifications known to those skilled in the art may be implemented without departing from the scope and spirit of the invention as recited in the claims below.